Findynet Osuuskunta

Teknologiafoorumi

7.3.2024 Samuel Rinnetmäki (Findynet), Petri Tillikainen ja Visa Varjus (Tietoevry)

Aiheena tänään

Suostumus lompakkosovelluksella

Findynet

Digitaalinen suostumus lompakkosovelluksella

1. Taustatietoa
2. Käyttötapaus
3. Suostumuksen antaminen sovelluksella
4. Teknologiat
5. Saavutettavat hyödyt
6. Haasteet
7. Ratkaisumallit

Taustatietoa

Findynet

Suostumus

- Suostumus tiedon jakamiseen eri toimijoiden välillä
- Käyttötarkoituksena pääosin ihmisten välinen tiedonvaihto

- Ei olla ratkaisemassa tietojärjestelmien välisten rajapintakutsujen luvitusta (siihen on jo OAuth)
- Ei olla antamassa valtuuksia tai valtakirjoja (tietoja vaihtavat toimijat eivät asioi tietojen kohteen puolesta)

> ”
>
> Nämä terveydenhuollon, sosiaalihuollon ja sosiaaliturvan toimijat saavat vaihtaa tietoja tilanteestani
>
> ”

Taustaa

- Ongelma: suostumusten antamiseen ei ole helppoa ja luotettavaa tapaa.
- Hypoteesi: suostumuksen voisi antaa lompakkosovelluksella
- Suunniteltiin ratkaisu käyttäjäkeskeisesti
- Toteutettiin Figma-prototyyppi
- Rajauduttiin suostumuksen antamiseen – suostumuksen hyödyntämistä on suunniteltu, mutta ei mukana prototyypissä

Findynet

Käyttötapaus

Suostumusprosessi

- Suostumuspyynnön luominen palvelussa
- Sovelluksen avaaminen
- Suostumuksen hyväksyminen tai hylkääminen
- Suostumus-todisteen välittäminen
- Suostumusten selaaminen ja muokkaaminen

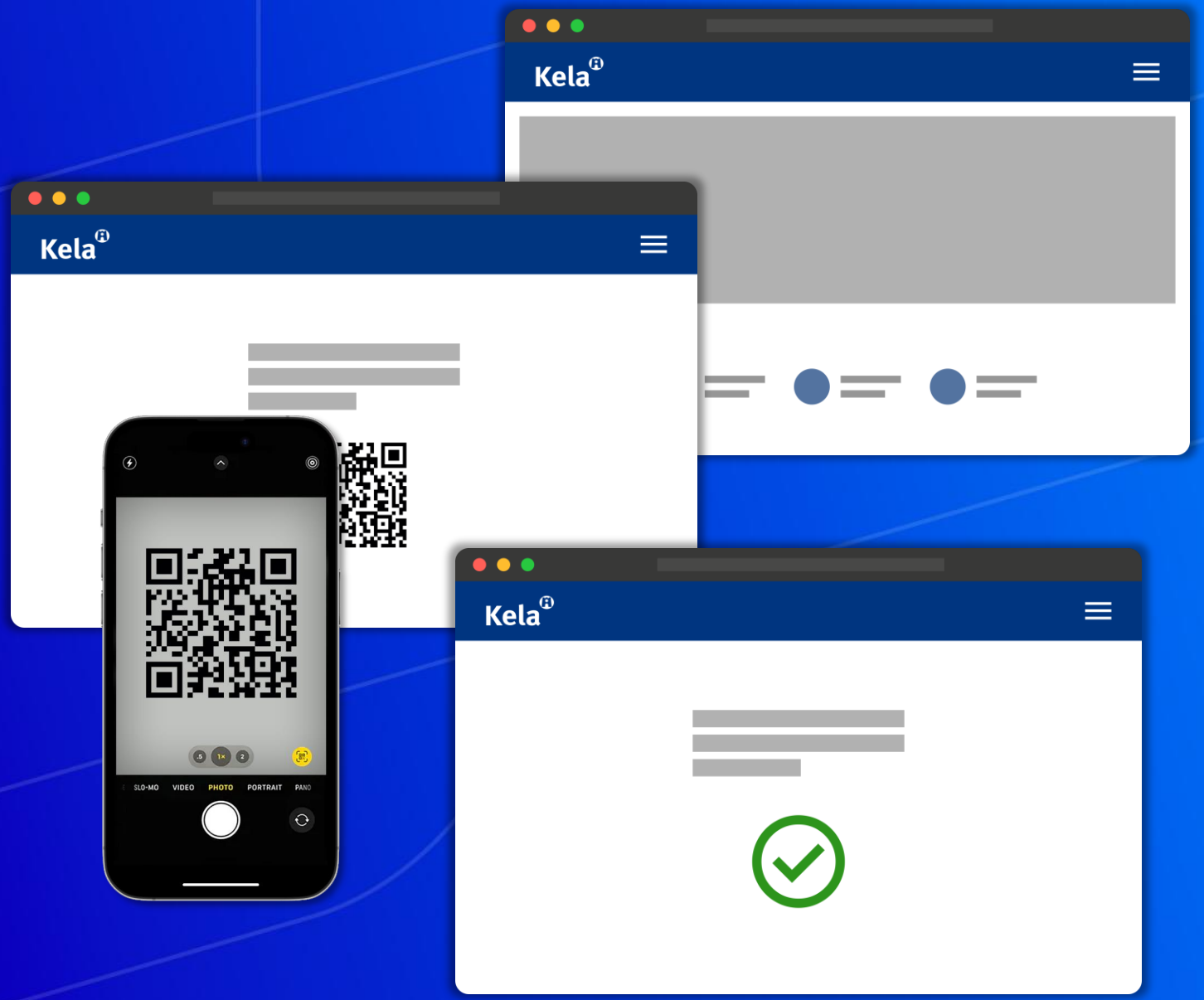
Vaihe vaiheelta

Suostumuksen antaminen sovelluksella

Findynet

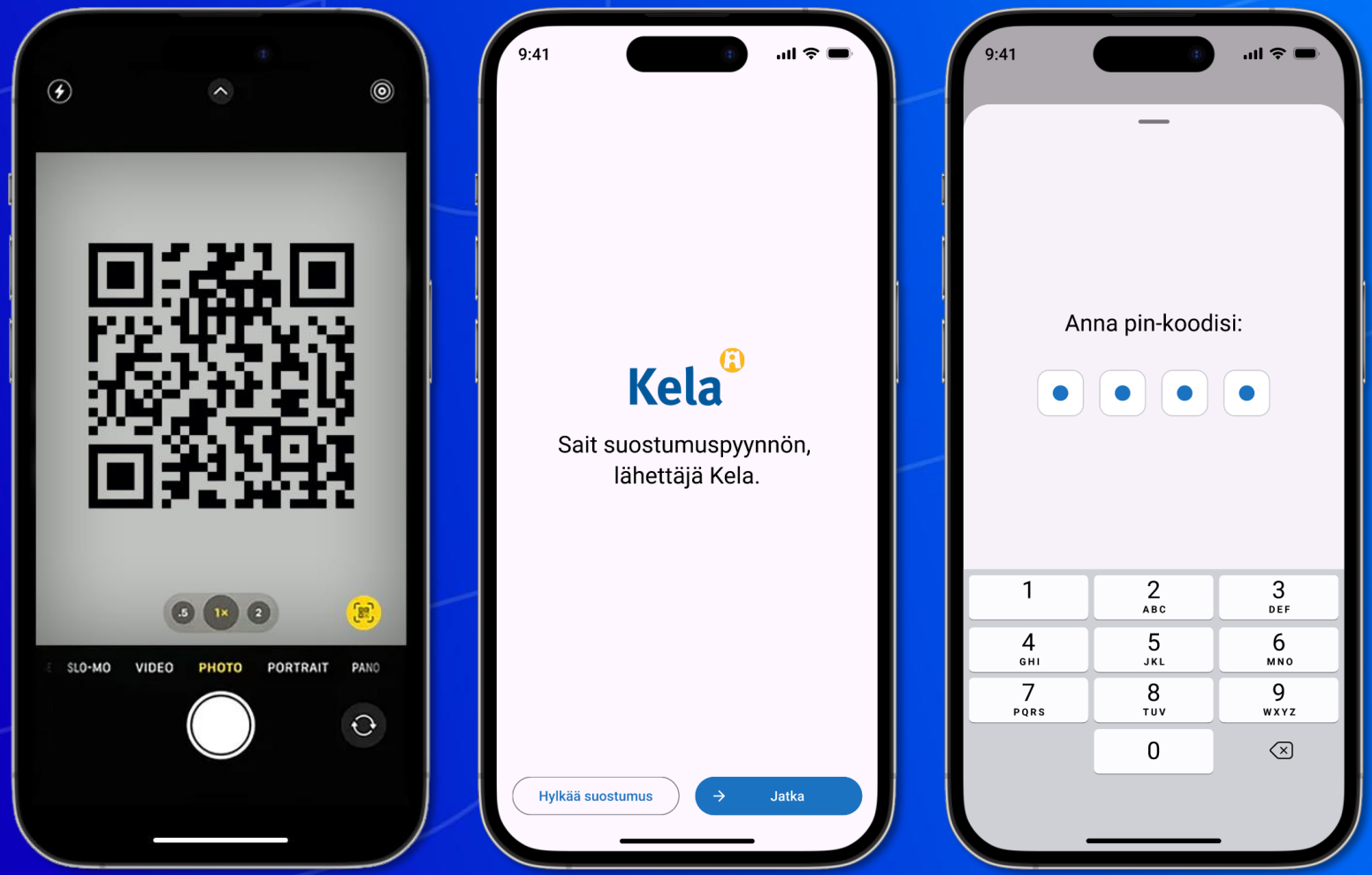
Pyyntö antaa suostumus

1. Käyttäjä menee palveluun (tässä omakela.fi) ja aloittaa palveluprosessin
2. Palvelussa käyttäjä saa QR-koodin tai linkin, jonka avulla hän voi avata suostumuspyynnön lompakkosovelluksella



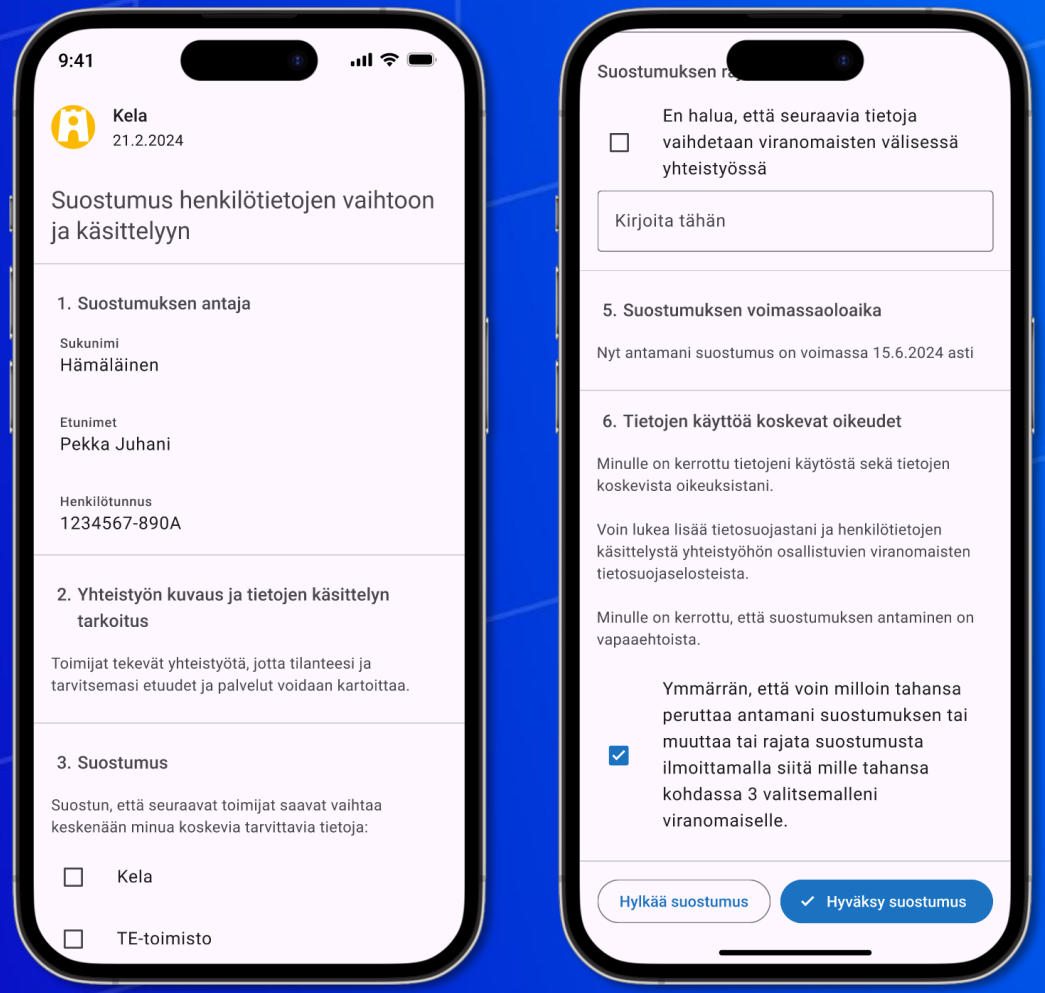
Sovelluksen avaaminen ja kirjautuminen

1. Käyttäjä skannaa QR-koodin ja sovellus aukeaa
2. Lompakkosovellus näyttää suostumuspyynnön, jonka voi joko hyväksyä tai hylätä
3. Käyttäjä kirjautuu sovellukseen sovelluskohtaisella pin-koodilla



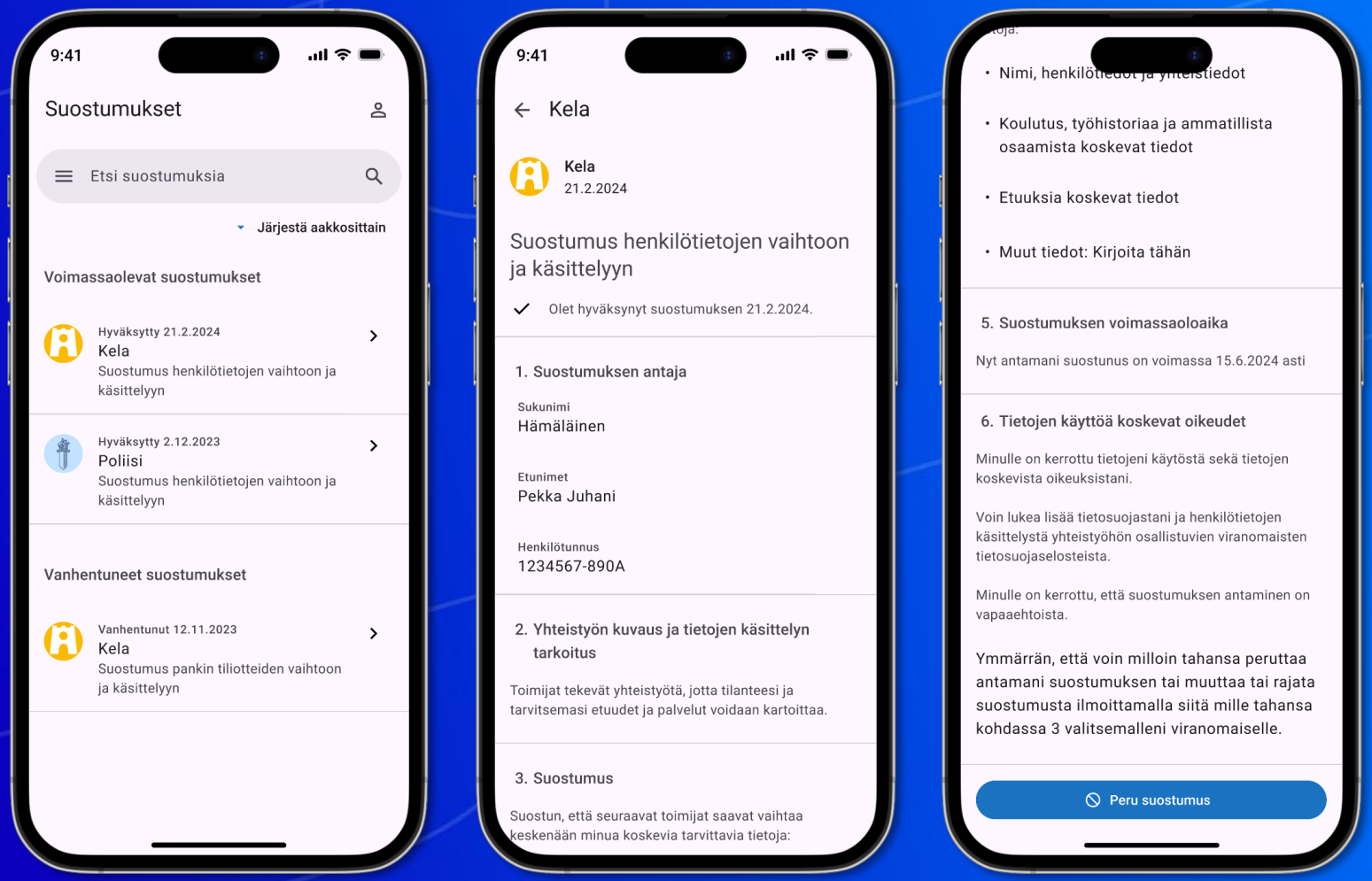
Suostumuksen hyväksyminen tai hylkääminen

1. Käyttäjä tarkastaa pyynnön ja tekee valintoja
2. Lopuksi käyttäjä hyväksyy tai hylkää suostumuksen



Suostumusten selaaminen ja muokkaaminen

1. Kaikkia suostumuksia voi selata
   - Hakutoiminnolla
   - Listaamalla suostumukset aakkosittain tai aikajärjestykseen
2. Voimassaolevan suostumuksen voi perua, mutta peruttua suostumusta ei voi palauttaa hyväksytyksi. (Annettava uusi suostumus.)



Miltä suostumuksen antaminen näyttäisi

Kaksi esimerkkiä

Findynet

Suostumus henkilötietojen vaihtoon ja käsittelyyn

Suostumuksen hyväksyminen

Käyttäjä valitsee tahot, jotka saavat vaihtaa tietoja suostumuksen perusteella.

Findynet

Suostumus tilitietojen saamiseen pankista

Yksinkertainen suostumuksen antaminen

Suostumuksen peruminen myöhemmin

Findynet

Digitaalisen suostumuksen antamiseen soveltuvat

Teknologiat

Findynet

Lähtöolettama

- Suostumuspyyntö voi olla mikä tahansa dokumentti,
  - jonka sovellus osaa näyttää käyttöliittymässä
  - ja jolle sovellus osaa tarjota vaaditut muokkaustoiminnot.
- Lompakkosovellus muodostaa suostumuksesta todisteen, jonka se välittää suostumusta pyytäneelle palvelulle.

Soveltuvat teknologiat

- Eurooppalaisella identiteettilompakolla voi tehdä sähköisen allekirjoituksen
- **Tai** lompakkosovellus voisi luoda (*self-issued*) suostumustodisteen allekirjoittamalla muokatun suostumuspyynnön
  - Suostumustodiste sekä vaadittavat henkilötiedot olisi mahdollista välittää esimerkiksi SIOPv2 + OpenID4VP -mekanismilla
  - SIOPv2 vaatisi suostumustarkoitukseen tehdyn laajennuksen, jonka avulla sovellus tunnistaisi SIOPv2 pyynnön käsittelevän suostumusta. Vertaa esim. OIDC Signature Extension
- Peruminen vaatisi revokaatiomekanismin.
  - Esim. Token Status List

Digitaalisten suostumusten avulla

Saavutettavat hyödyt

Findynet

Digitaalisten suostumusten hyötyjä

- Digitaalista suostumusta on lähes mahdoton väärentää (vrt. paperilla tai puhelimessa annettava suostumus)
- Suostumuksesta syntyy todennettava dokumentti, joka voidaan jakaa eri osapuolille tai tallentaa keskitetysti.
- Kuka tahansa voi tarkastaa suostumuksen sisällön ja voimassaolon.
- Suostumus jää myös sen antajan tietoon lompakkosovellukseen, josta se on peruttavissa helposti.

Digitaalisten suostumusten toteutuksen

Haasteet

Findynet

Haasteita ja ratkottavia asioita

- Suostumuksen antajan yksilöinti
  - `"iss": "did:key:F00843-69402-…?"`
- Revokointi lompakkosovelluksesta
  - Tuleeko lompakkosovelluksiin toimintoja todisteiden myöntämiseen ja revokointiin?
  - Sähköisen allekirjoituksen revokointi?
- Suostumuksen antaminen usealle osapuolelle kerralla
  - Suostumuksen ensimmäinen vastaanottaja jakaa sen muille osapuolille?
  - Tallennus keskitettyyn rekisteriin?
- "Vapaamuotoisen", suostumuksen hyödyntäminen osana automaatiota voi olla hankalaa
  - Järjestelmien välisten rajapintojen luvitukseen Oauth lienee parempi ratkaisu

Vaihtoehtoinen ratkaisumalli

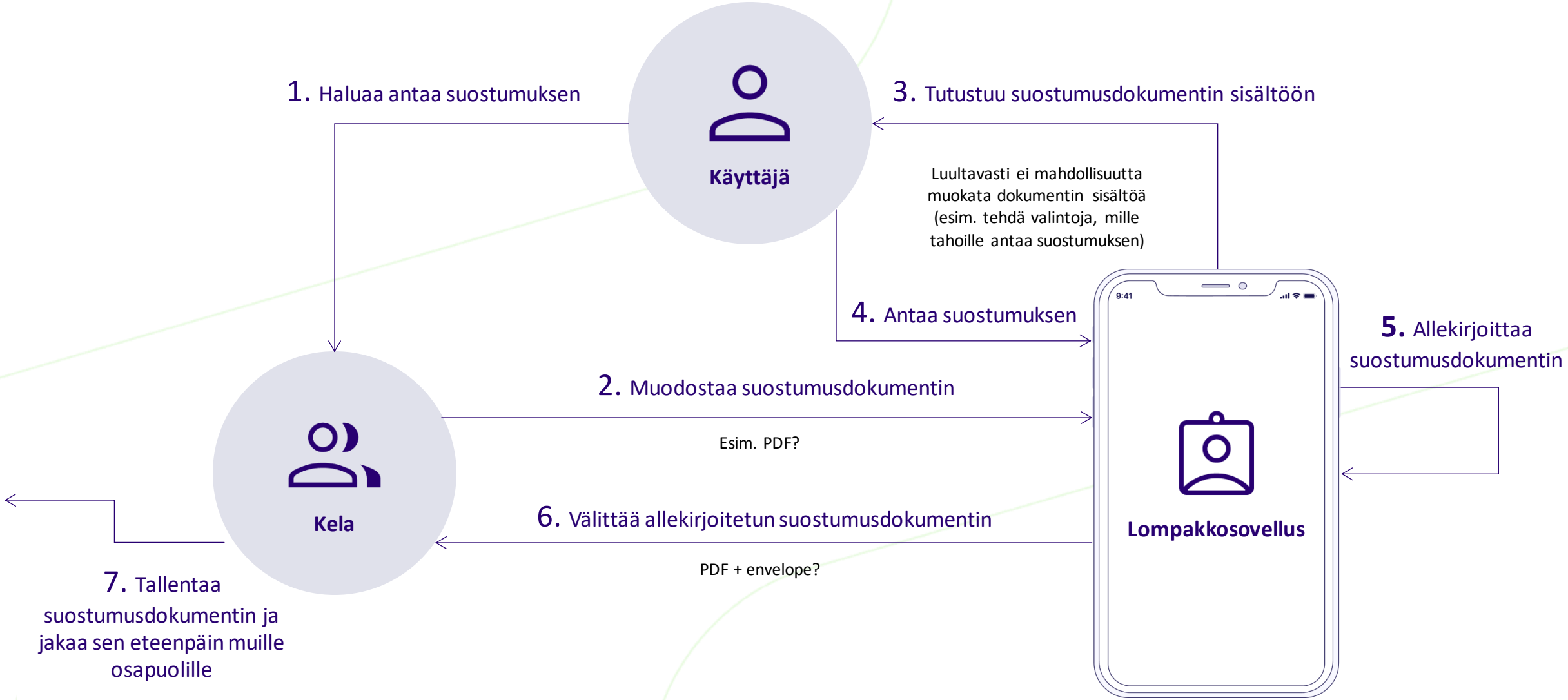
- Kun suostumusta pyydetään kolmannen osapuolen tarjoamaan rajapintaan (esim. tiliotteet tai -tapahtumat)
- Tilitietojen hakemiseen lienee mahdollista käyttää Open Banking -rajapintoja
- Suostumuspyynnön käsittelijänä toimisi resurssin tarjoava taho (pankki)

Digitaalisen suostumuksen

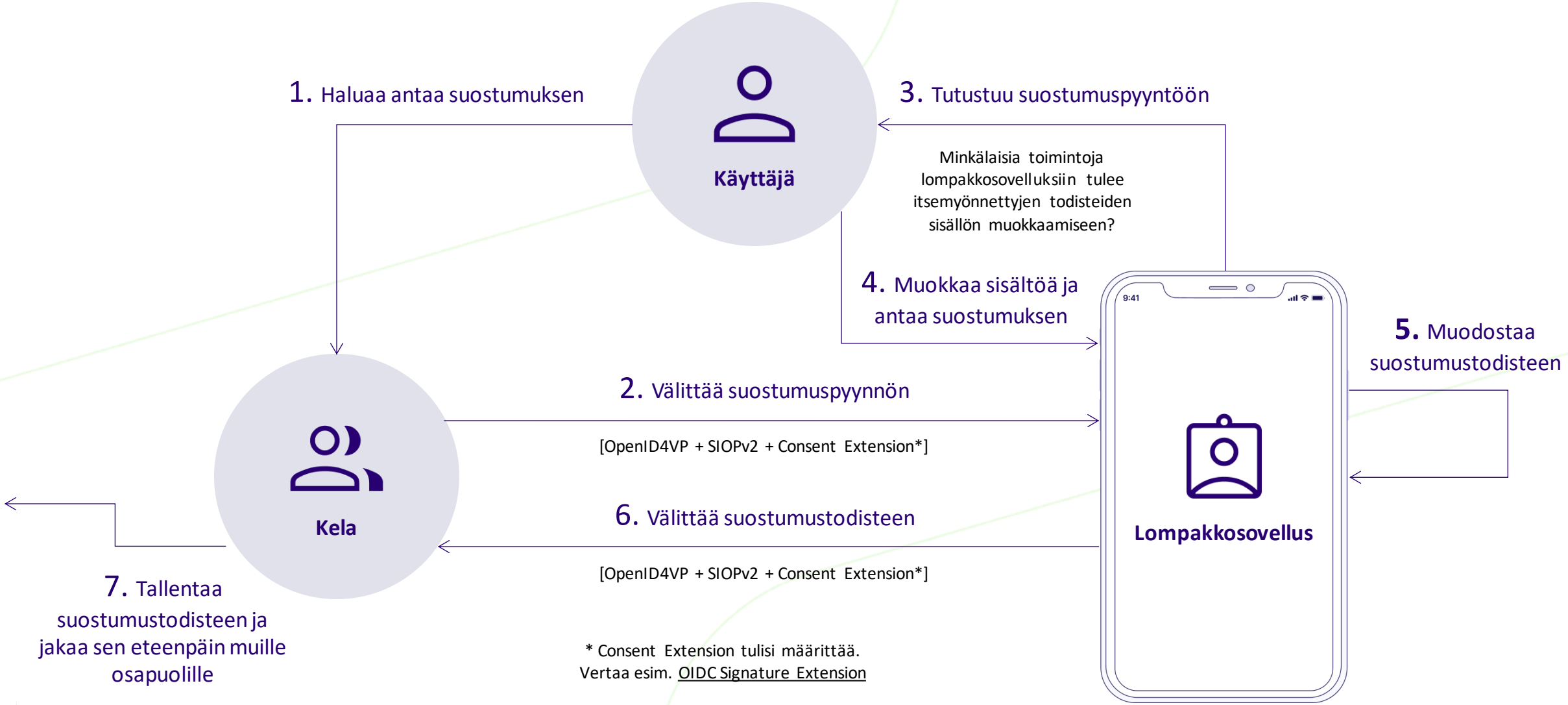
Ratkaisumallit

Findynet

Sähköinen allekirjoitus lompakkosovelluksella



OpenID4VP + SIOPv2 + Consent Extension (TBD)



Kiitos!

Kommentteja?

Kysymyksiä?

Findynet